APPENDIX A

DEFINITIONS AND ABBREVIATIONS

Access - The ability and opportunity to obtain knowledge or possession of classified information.

Agency - Any "Executive agency," as defined in 5 U.S.C., 105; any "Military Department" as defined in 5 U.S.C. 102; and any other entity within the Executive Branch that comes into the possession of classified information. The DON is an agency but each DON command is not; rather, a command is part of an agency, the DON. Within the DoD, the Departments of the Army, Navy, and Air Force are agencies.

Assist Visit - The informal assessment of the security posture of a command to be used as a self-help tool.

Associated Markings - The classification authority, office of origin, warning notices, intelligence and other special control markings, and declassification/downgrading instructions of a classified document.

Automatic Declassification - The declassification of information based upon the occurrence of a specific date or event as determined by the OCA or the expiration of a maximum time for duration of classification established under E.O. 12958.

Automated Information System (AIS) - An assembly of computer hardware, software, or firmware configured to collect, create, compute, communicate, disseminate, process, store, or control data or information.

Carve-Out - A classified contract issued in connection with an approved SAP in which the DSS has been relieved of inspection responsibility in whole or in part under the NISP.

Classification - The determination by an authorized official that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure.

Classification Authority - The authority by which information is classified (see OCA).

Classification Guide - See Security Classification Guide.

Classification Management - The management of the life cycle of classified information from its inception to its eventual declassification or destruction.

Classified Contract - Any contract that requires or will require access to classified information by a contractor or its employees in the performance of the contract.

Classified National Security Information (or "Classified Information") - Information that has been determined to require protection against unauthorized disclosure in the interest of national security and is classified for such purpose by appropriate classifying authority per the provisions of E.O. 12958 or any predecessor Order.

Classified Material - Any matter, document, product or substance on or in which classified information is recorded or embodied.

Classifier - An approved official who makes a classification determination and applies security classification to information. A classifier may be an approved OCA, designated in **exhibit 4A**, or a derivative classifier who assigns a security classification based on a properly classified source or classification guide.

Cleared Contractor - Any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government and granted an FCL by the CSA for the purpose of performing on a classified contract, license, IR&D program, or other arrangement that requires access to classified information.

Cleared DoD Contractor Employee - As a general rule, this term encompasses all contractor employees granted a personnel security clearance under the NISP. The requirements prescribed for a cleared contractor employee should be interpreted to include, as appropriate, company officers, consultants, employees issued an LAA, and employees possessing contractor-granted Confidential clearances.

Code Word - A single classified word assigned a classified meaning by an appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified Confidential or higher.

Cognizant Security Agency - Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry.

Cognizant Security Office (CSO) - See Operating Location (OPLOC).

Collateral Information - Information identified as NSI under the provisions of E.O. 12958 but which is not subject to enhanced security protection required for SAP or other compartmented information.

Command - For the purpose of this regulation, any organizational entity under one official authorized to exercise direction and control. The term includes, base, station, unit, laboratory, installation, facility, activity, detachment, squadron, and ship.

Commanding Officer - For the purpose of this regulation, the head of any DON organizational entity. The term includes commander, commanding general, director, and officer in charge, and any other title assigned to an official, military or civilian, who, through command status, position or administrative jurisdiction, has the authority to render a decision with regard to a specific question under consideration.

Communications Security (COMSEC) - The protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. COMSEC includes: (1) Cryptosecurity, which results from providing technically sound cryptosystems and their proper use; (2) Physical security, which results from physical measures taken to safeguard COMSEC material; (3) Transmission security, which results from measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis; and (4) Emission security, which results from measures taken to deny unauthorized persons information of value which might be derived from the interception and analysis of compromising emanations from cryptoequipment and telecommunications system.

Compromise - An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance.

Confidential Source - Any individual or organization that has provided, or may provide, information to the U.S. on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Consignee - A person, firm, or government named as the receiver of a shipment; one to whom a shipment is consigned.

Consignor - A person, firm or government activity by whom articles are shipped. The consignor is usually the shipper.

Constant Surveillance Service (CSS) - A transportation protective service provided by a commercial carrier qualified by the MTMC to transport Confidential shipments.

Continental United States (CONUS) - United States territory, including adjacent territorial waters, located within the North America continent between Canada and Mexico.

Contracting Command - A DON command with procurement authority to award contracts to industry.

Contracting Officer - A Government official, who, per the departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representatives of the contracting officer, acting within the limits of their authority.

Contracting Officer's Representative (COR) - A security specialist at a DON contracting command who has been appointed a COR and delegated authority on behalf of the command for the security administration of classified contracts. The COR serves as the responsible official for any problems or questions related to security requirements and/or classification guidance for classified contracts (formerly known as Contracting Officers Security Representative).

Controlled Cryptographic Item - A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified but controlled.

Controlled Unclassified Information - Official information not classified or protected under E.O. 12958 or its predecessor orders that requires the application of controls and protective measures for a variety of reasons.

Counterintelligence (CI) - Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine activities, sabotage, international terrorist activities, or assassinations.

Critical Nuclear Weapons Design Information (CNWDI) - Top Secret or Secret RD revealing the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, and high explosive material by type. Among these excluded items are the components which personnel set, maintain, operate, test, or replace.

Critical Technology - Technology that consists of: (1) Arrays of design and manufacturing know-how (including technical data); (2) keystone manufacturing, inspection, and test equipment; (3) keystone materials; and (4) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the U.S. (also referred to as militarily critical technology).

Cryptanalysis - The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system of key employed in the encryption.

Cryptography - The branch of cryptology that treats the principles, means, and methods of designing and using cryptosystems.

Cryptology - The branch of knowledge that treats the principles of cryptography and cryptanalysis; and the activities involved in SIGINT and maintaining COMSEC.

Custodial Responsibility - The command which has classified information, or is charged with responsibility for its safeguarding, at the time of its loss or compromise.

Custodian or Custodial Command - The individual or command who has possession of, or is otherwise charged with the responsibility for safeguarding classified information.

Damage to the National Security - Harm to the national defense or foreign relations of the U.S. resulting from the unauthorized disclosure of classified information.

Declassification - The determination by an authorized official that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure.

Declassification Authority - The official who authorizes original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority, in writing, by the agency head or the senior agency official.

Deliberate Compromise - Any intentional act of conveying classified information to any person not officially authorized to receive it.

Derivative Classification - The incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and ensuring that it continues to be classified by marking or similar means when included in newly created material.

Disclosure - Conveying classified information to another person.

Document - Any physical medium such as any publication (bound or unbound printed material such as reports, studies, manuals), correspondence (such as military and business letters and memoranda), electronic media, audio-visual material (slides, transparencies, films), or other printed or written products (such as charts, maps) on which information is recorded or stored.

DoD Component - The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the Defense agencies.

Downgrading - The determination by an approved authority that information classified at a specific level requires a lower degree of protection, therefore, reducing the classification to a lower level.

Event - An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification or downgrading of information.

Exception - A written, CNO (N09N2)-approved long-term (36 months or longer) or permanent deviation from a specific safeguarding requirement of this regulation. Exceptions require compensatory security measures.

Facility Security Clearance (FCL) - An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

File Series - Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Foreign Government - Any national governing body organized and existing under the laws of any country other than the U.S. and its possessions and trust territories and any agent or instrumentality of that government.

Foreign Government Information (FGI) - Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; information produced by the U.S. under or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or information received and treated as FGI under the terms of a predecessor order to E.O. 12958.

Foreign Intelligence - The product from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power and which is significant to the national security, foreign relations, or economic interests of the U.S. and which is provided by a Government agency that is assigned an intelligence mission.

Foreign National - Any person not a U.S. citizen, U.S. national, or immigrant alien. American citizens representing foreign governments, foreign private interests, or other foreign nationals are considered to be foreign nationals for purposes of this regulation, when acting in that capacity.

Foreign Recipient - A foreign government or international organization, to whom the U.S. is providing classified information.

Formerly Restricted Data (FRD) - Information removed from the DOE RD category upon a joint determination by the DOE (or antecedent agencies) and the DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as RD.

Government-to-Government - Transfers by Government officials through official channels or through other channels specified by the governments involved.

Industrial Security - That portion of information security which is concerned with the protection of classified information entrusted to U.S. industry.

Information - Any official knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Security - The system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information Systems Security (INFOSEC) - The protection of information systems against unauthorized access to or the modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Information Systems Security Manager (ISSM) - A person responsible for developing, maintaining, and directing the implementation of the INFOSEC program within the command. The ISSM advises the commanding officer on all INFOSEC matters, including identifying the need for additional INFOSEC staff. Serves as the command's point of contact for all INFOSEC matters and implements the command's INFOSEC program (Previously the ADP systems security officer (ADPSSO)).

Information Systems Security Officer (ISSO) - A person(s) responsible for implementing and maintaining the command's information system and network security requirements.

Infraction - Any knowing, willful, or negligent action contrary to the requirements of E.O. 12958 or its implementing directives that does not comprise a "violation."

Inspection - An official examination of the security posture of a command to determine compliance with ISP policy.

Intelligence - The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

Intelligence Activity - An activity that an agency within the intelligence community is authorized to conduct under E.O. 12333.

Intelligence Community - U.S. organizations and activities identified by E.O. 12333 as making up the Community. The following organizations currently comprise the Intelligence Community: CIA; NSA; DIA; special offices within the DoD for the collection of specialized foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the DOS; the intelligence elements of the military services, FBI, DEA, Departments of Treasury and Energy and the DEA; and staff elements of the Office of the DCI.

Interim Top Secret Facility Clearance - Clearance granted by DSS/ OCC following authorization by a U.S. Government activity to avoid crucial delays in precontract or contract negotiations, the award of a contract, or performance on a contract.

Inventory - The process of accounting for classified information.

Interagency Security Classification Appeals Panel (ISCAP) - A panel that will (1) decide on appeals by persons who have filed classification challenges; (2) approve, deny, or amend agency exemptions for automatic declassification; and (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review.

Judge Advocate General (JAG) Manual Investigation - A proceeding conducted per chapter II of the Manual of the Judge Advocate General. It is usually ordered by the command having custodial responsibility for the classified information which has been compromised or subjected to compromise.

Mandatory Declassification Review - Review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of E.O. 12958.

Marking - The physical act of indicating on classified material the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on the use of the classified information.

Multiple Sources - Two or more source documents, classification guides, or a combination of both.

National Industrial Security Program (NISP) - National program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government and serves as a single, integrated, cohesive industrial security program to protect classified information and preserve U.S. economic and technological interests.

National Security - The national defense or foreign relations of the U.S.

National Security Information (NSI) - Any official information that has been determined under E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is so designated. The designations Top Secret, Secret, and Confidential are used to identify such information and are usually referred to as "classified information."

Naval Nuclear Propulsion Information (NNPI) - All information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and naval nuclear power plant prototypes, including the associated nuclear support facilities.

Need-to-know - A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized U.S. Governmental function.

Network - A system of two or more computers that can exchange data or information.

Nickname - A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

Official Information - Information which is owned by, produced for or by, or is subject to the control of the U.S. Government.

Operating Location (OPLOC) - A DSS office that provides administrative assistance and policy guidance to local DSS field elements charged with security oversight of cleared DoD contractors performing on classified contracts.

Original Classification - An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority (OCA) - An official authorized in writing, either by the President, an agency head, or other official designated by the President "to classify information originally" or "to make an original classification decision."

Permanent Historical Value - Those records that have been identified in an agency's records schedule as being permanently-valuable.

Possessions - U.S. possessions are the U.S. Virgin Islands, Guam, American Samoa, Swain's Island, Howland Island, Baker Island, Jarvis Island, Midway Islands (this consists of Sand Island and Eastern Island), Kingman Reef, Johnston Atoll, Navassa Island, Swan Island, Wake Island, and Palmyra Island.

Preliminary Inquiry (PI) - The "initial" process to determine the facts surrounding a possible loss or compromise. A narrative of the PI findings are required when there is a loss or compromise of classified information.

Program Manager - Senior level official responsible for managing all aspects of development, production, and delivery related to an acquisition program. Develops program strategies and identifies industry roles and requirements in support of their programs.

Program Review - Formal assessment of the security posture of a command to be used in improving the management of the ISP.

Protective Security Service (PSS) - A transportation protective service provided by a cleared commercial carrier qualified by the MTMC to transport Secret material.

Qualified Contractor - A private individual or enterprise located in the U.S. or Canada whose eligibility to obtain unclassified export controlled technical data has been established following certification of an Export-Controlled DoD and Canada Technical Data Agreement, DD 2345.

Record - All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any command of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that command or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the information value of data in them.

Regrade - To raise or lower the classification assigned to an item of information.

Report of Investigation (ROI) - Official report of investigation conducted by agents of the NCIS.

Restricted Data (RD) - All data concerning: (1) Design, manufacture, or utilization of atomic weapons; (2) The production of special nuclear material; or (3) The use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category under Section 142 of the AEA, as amended.

Risk Management - The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

Safeguarding - Measures and controls prescribed to protect classified information.

Security Classification Guide (SCG) - The primary reference source for derivative classifiers to identify the level and duration of classification for specific informational elements. DON OCAs are required to prepare an SCG for each system, plan, program or project under their cognizance which creates classified information.

Security-In-Depth - A determination by the commanding officer that a command's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the command. Examples include perimeter fences, employee and visitor access controls, use of IDSs, random guard patrols during non-working hours, closed circuit video monitoring, and other safeguards that reduce the vulnerability of unalarmed storage areas and security storage cabinets.

Self-Inspection - The internal review and evaluation of a command or the DON as a whole with respect to the implementation of the program established under E.O. 12958 and its implementing directives.

Senior Agency Official (SAO) - The official designated by the agency head under section 5.6(c) of E.O. 12958 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Sensitive But Unclassified (SBU) - Information that is originated within the DOS and warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the FOIA. (Previously "Limited Official Use" (LOU) in the DOS).

Sensitive Information (Computer Security Act of 1987) - Certain information in Federal Government AISs defined as "Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5 U.S.C. (Privacy Act), but which has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

Sensitive Compartmented Information (SCI) - Classified information concerning or derived from intelligence sources or methods, or analytical processes, that is required to be handled within formal access control systems established by the DCI.

Short Title - A brief, identifying combination of words, letters, or numbers applied to specific items of classified information.

Signals Intelligence (SIGINT) - Intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

Single Integrated Operational Plan (SIOP) - A general war plan of the Joint Chiefs of Staff distributed by the Joint Staff Director of Strategic Target Planning.

Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) - Detailed Top Secret SIOP information that is extremely sensitive in nature.

Source Document - An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP) - Any DoD program or activity (as authorized in E.O. 12958) employing enhanced security measures (e.g., safeguarding or personnel adjudication requirements) exceeding those normally required for classified information at the same classification level which is established, approved, and managed as a DoD SAP.

Systematic Declassification Review - The review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. to have permanent historical value per Chapter 33 of Title 44, U.S.C.

Technical Data - Recorded information related to experimental or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Examples of technical data include research and engineering data or drawings, associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentation.

Technical documents - Documents containing technical data or information.

Technical Information - Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

Telecommunications - The preparation, transmission, or communication of information by electronic means.

Transmission - Any movement of classified information from one place to another.

Transportation - A means of transport; conveyance of classified equipment or bulky shipments.

Unauthorized Disclosure - A communication or physical transfer of classified information to an unauthorized recipient.

Unclassified Controlled Nuclear Information (UCNI) - DoD or DOE unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material, equipment or facilities.

U.S. and its Territorial Areas - The 50 states, the District of Columbia, the Commonwealth of PR, and those possessions listed in the definition above.

U.S. Citizens (including U.S. Nationals) - A person born in one of the 50 States, its territories, possessions, Administrative and Commonwealth Areas, the DC, PR, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the U.S.). Naturalized U.S. citizen, or person born abroad of U.S. parent(s) and registered with an appropriate authority (U.S. Consul, DOS). For the purpose of the issuance of personnel security clearances, citizens of the Federated States of Micronesia and the Republic of the Marshall Islands are considered U.S. citizens.

Upgrade - To raise the classification of an item of information from one level to a higher one.

Visitor Group - Cleared DoD contractor employees assigned to a DON command, normally in support of a classified contract or program, who occupy or share Government spaces for a predetermined period.

Waiver - A written temporary relief, normally for a period of 1 year, from specific requirements imposed by this regulation, pending completion of actions which will result in conformance with the requirements. Interim compensatory security measures are required.

ABBREVIATIONS

ACS - Access Control System

AIS - Automated Information System

AEA - Atomic Energy Act

AECS - Access Entry Control Systems

C - Confidential

CI - Counterintelligence

CIA - Central Intelligence Agency

CHINFO - Chief of Information

CMC - Commandant of the Marine Corps

CMS - Communications Security Material System

CNO - Chief of Naval Operations

CNR - Chief of Naval Research

CNWDI - Critical Nuclear Weapons Design Information

CO - Commanding Officer

COMNAVSECGRU - Commander, Naval Security Group

COMSEC - Communications Security

COR - Contracting Officer's Representative (formerly Contracting Officer's Security Representative)

CSA - Cognizant Security Agency

CSP - Cryptographic Security Publication

CSS - Constant Surveillance Service

CUSR - Central U.S. Registry (NATO)

CVA - Central Verification Activity

DASD(S&IO) - Deputy Assistant Secretary of Defense, Security and Information Operations

DCI - Director, Central Intelligence

DCID - Director, Central Intelligence Directive

DCMS - Director, Communications Security Material System

DCS - Defense Courier Service

DEA - Drug Enforcement Agency

DIA - Defense Intelligence Agency

DLSC - Defense Logistics Services Center

DNI - Director of Naval Intelligence

DoD - Department of Defense

DODDAC - Department of Defense Damage Assessment Committee

DOE - Department of Energy

DON - Department of the Navy

DOS - Department of State

DSS - Defense Security Service (formerly Defense Investigative Service)

DTS - Defense Transportation System

DUSD(PS) - Deputy Under Secretary of Defense for Policy Support

E.O. - Executive Order

ESS - Electronic Security System

FAA - Federal Aviation Administration

FAD - Facility Access Determination

FBI - Federal Bureau of Investigation

FCL - Facility (Security) Clearance

FEDEX - Federal Express

FGI - Foreign Government Information

FI - Foreign Intelligence

FMS - Foreign Military Sales

FIPS - Federal Information Processing Standard

FOIA - Freedom of Information Act

FOUO - For Official Use Only

FRD - Formerly Restricted Data

GAO - General Accounting Office

GSA - General Services Administration

IC - Intelligence Community

IDE - Intrusion Detection Equipment

IDS - Intrusion Detection Systems

INFOSEC - Information Systems Security

IR&D - Independent Research and Development

ISP - Information Security Program

ISOO - Information Security Oversight Office

ISSM - Information Systems Security Manager

ISSO - Information Systems Security Officer

ITAR - International Traffic in Arms Regulation

JAG - Judge Advocate General of the Navy

JANAP - Joint Army, Navy, Air Force Publication

JCS - Joint Chiefs of Staff

LAA - Limited Access Authorization

MTMC - Military Traffic Management Command

NARA - National Archives and Records Administration

NATO - North Atlantic Treaty Organization

NAVY IPO - Navy International Programs Office

NCIS - Naval Criminal Investigative Service (Formerly NSIC, NISCOM and NIS)

NCISFO - Naval Criminal Investigative Service Field Office

NCISRA - Naval Criminal Investigative Service Resident Agency

NISP - National Industrial Security Program

NISPOM - National Industrial Security Program Operating Manual

NNPI - Naval Nuclear Propulsion Information

NSA - National Security Agency

NSG - Naval Security Group

NSN - National Stock Number

NWP - Naval Warfare Publication

OASD(C^3I) - Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

OASD(PA) - Office of the Assistant Secretary of Defense (Public Affairs)

OCA - Original Classification Authority

OCC - Operations Center Columbus (formerly Defense Investigative Service Clearance Office (DISCO))

ONI - Office of Naval Intelligence

OPLOC - Operating Location (formerly Cognizant Security Office)

OSD - Office of the Secretary of Defense

PA - Privacy Act

PAO - Public Affairs Officer

PCL - Personnel Clearance Level

PCU - Premise Control Unit

PI - Preliminary Inquiry

PIN - Personal Identification Number

PM - Program Manager

POE - Port of Embarkation

PPP - Program Protection Plan

PRIN DIR (S&IO) - Principal Director, Security and Information Operations

PSS - Protective Security Service

RANKIN - Retrieval and Analysis of Navy Classified Information

RD - Restricted Data

ROI - Report of Investigation

S - Secret

SAC - Special Agent in Charge

SAO - Senior Agency Official

SAP - Special Access Programs

SBU - Sensitive But Unclassified

SCG - Security Classification Guide

SCI - Sensitive Compartmented Information

SCIF - Sensitive Compartmented Information Facility

SECDEF - Secretary of Defense

SECNAV - Secretary of the Navy

SF - Standard Form

SIOP - Single Integrated Operationals Plan

SIOP-ESI - Single Integrated Operational Plan-Extremely Sensitive Information

SJA - Staff Judge Advocate

SOIC - Senior Official of the Intelligence Community

SSO - Special Security Officer

SSSO - Subordinate Special Security Officer

TS - Top Secret

TSCA - Top Secret Control Assistant

TSCO - Top Secret Control Officer

UCNI - Unclassified Controlled Nuclear Information

UIC - Unit Identification Code

USMTF - U.S. Message Text Format

U.S.C. - United States Code

USPS - United States Postal Service

USSAN - United States Security Authority, NATO